

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF:

Apple iPhone (white), seized on September 20, 2023, and listed as Exhibit L under Pittsburgh Bureau of Police (PBP) CCR 23-150035, currently in the custody of PBP at 1203 Western Ave, Pittsburgh, PA 15233

Magistrate No. 23-1527

Apple iPhone (black), seized on September 20, 2023, from the person of Smith and listed as Exhibit M under Pittsburgh Bureau of Police (PBP) CCR 23-150035, currently in the custody of PBP at 1203 Western Ave, Pittsburgh, PA 15233

Magistrate No. 23-1528

TCL “flip” cellular device, seized on September 20, 2023, and listed as Exhibit N under Pittsburgh Bureau of Police (PBP) CCR 23-150035, currently in the custody of PBP at 1203 Western Ave, Pittsburgh, PA 15233

Magistrate No. 23-1529

**AFFIDAVIT/APPLICATION IN SUPPORT OF SEARCH WARRANTS FOR
CELLULAR PHONES**

I, Marc Wilner, being first duly sworn, hereby state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms, & Explosives (“ATF”) and have been so employed since 2015. Prior to my employment with the ATF, I was employed as a Probation Officer with the Allegheny County Court of Common Pleas from 2008 to 2015. For over six (6) of those years, I served with the High Impact Unit of the Probation Office. This specialized unit dealt with probationers and parolees who had a high risk of

recidivism, such as drug dealers, violent offenders and gang members. I worked closely with the Pittsburgh Police Intelligence Unit (which tracked gang activity within the city of Pittsburgh) and the Allegheny County Sheriff's Office Fugitive Unit. I participated in numerous searches during my time with the Probation Office and many of them resulted in the seizure of guns and drugs. I am currently assigned to the Pittsburgh Field Office of the ATF.

2. I received extensive training at the Department of Homeland Security Criminal Investigative Training Program and the Bureau of Alcohol, Tobacco, Firearms and Explosives Special Agent Basic Training at the Federal Law Enforcement Training Center. This training lasted for over six (6) months and covered topics including federal criminal statutes, interviewing and interrogation techniques, arrest procedures, search and seizure, narcotics, undercover techniques, search warrant applications, and various other investigative techniques.

3. Throughout my career as an ATF Special Agent, I have been the affiant on numerous arrest warrants and search warrants to include search warrants for residences, vehicles, person, electronic devices, social media accounts, etc. I have also been a Case Agent and or Co-Case Agent in cases involving the illegal trafficking of firearms and narcotics, crimes of violence to include robbery, homicide and cases involving criminal groups and or gangs.

4. It should be noted that as a result of your Affiant's training and experience and your Affiant's conversations with prosecutors, your Affiant is aware that people who are involved in the illegal purchase/ possession of firearms, and the illegal possession of/distribution of narcotics, commonly store or retain evidence of their involvement on their cellular telephones, including but not limited to: incoming/outgoing call logs, contact lists, text messages, photographs, videos, and voicemails. This is true not just of criminals in general, but of individuals involved potential firearms and narcotics trafficking.

5. Such cellular telephone evidence can also include internet searches firearms, ammunition, and the components of firearms, as well as incriminating communications via emails or instant messages involving narcotics trafficking, such as the “stamp” of heroin being sold. Narcotics traffickers often the “stamp” which is found on a bag/dose of heroin, as a “brand” for the narcotic they are currently distributing. It should be noted that, with the advance of technology, the distinction between computers and cellular telephones is quickly becoming less clear. Actions such as internet searching or emailing, in addition to calling and text messaging, can now be performed from many cell phones. In addition, those involved in firearms possession/trafficking crimes commonly communicate using cellular telephones and computers.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

6. This affidavit application is submitted pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the following cellular telephone:

- Apple iPhone (white), seized on September 20, 2023, and listed as Exhibit L under Pittsburgh Bureau of Police (PBP) CCR 23-150035, currently in the custody of PBP at 1203 Western Ave, Pittsburgh, PA 15233 (hereinafter, **DEVICE 1**)
- Apple iPhone (black), seized on September 20, 2023, and listed as Exhibit M under Pittsburgh Bureau of Police (PBP) CCR 23-150035, currently in the custody of PBP at 1203 Western Ave, Pittsburgh, PA 15233 (hereinafter, **DEVICE 2**)
- TCL “flip” cellular device, seized on September 20, 2023, and listed as Exhibit N under Pittsburgh Bureau of Police (PBP) CCR 23-150035, currently in the custody of PBP at 1203 Western Ave, Pittsburgh, PA 15233 (hereinafter,

DEVICE 3)

7. **DEVICE 1, DEVICE 2, DEVICE 3** (referred to collectively herein as “**THE DEVICES**”) are currently in the custody of PBP at PBP Headquarters, located at 1203 Western Ave, Pittsburgh, PA 15233.

8. The search warrant that I am applying for would authorize the forensic examination of **THE DEVICES** for the purpose of identifying electronically stored data, described in Attachment A.

9. As explained below, there is probable cause to conclude that **THE DEVICES** contains evidence of the commission of the federal felony offenses 18 USC § 922(g)(1), 18 USC § 924(c) and 21 USC § 841 (a)(1) (“**TARGET OFFENSES**”), as listed in Attachment A. I have discussed this case with, and reviewed the reports of, other law enforcement officers who have been involved in this investigation.

10. This affidavit is being submitted for the specific purpose stated herein. I have not, therefore, included every fact known to me concerning this investigation. As further explained below, **THE DEVICES** were obtained by the Pittsburgh Bureau of Police as detailed below.

PROBABLE CAUSE

11. On September 20, 2023, investigators with the Pittsburgh Bureau of Police Fugitive Apprehension Unit (“PBP-FAU”) were conducting a fugitive investigation into Miquan MORGAN-GRAHAM (“MORGAN-GRAHAM”). MORGAN-GRAHAM had an active arrest warrant for Fleeing/Attempting to Elude Police, issued by the Allegheny County Court of Common Pleas.

12. PBP-FAU developed information that MORGAN-GRAHAM was residing in the area of Fleming Avenue in the North Side area of Pittsburgh. On September 20, 2023, investigators were conducting surveillance in the area, and observed MORGAN-GRAHAM exit an apartment building and get into an Uber vehicle. The Uber vehicle then began driving away.

13. Investigators maintained visual contact with the Uber. Shortly thereafter, investigators initiated a traffic stop of the Uber for the purposes of arresting MORGAN-GRAHAM for his outstanding state arrest warrant.

14. MORGAN-GRAHAM was in the rear of the vehicle and, other than the Uber driver, he was the sole occupant of the vehicle.

15. PBP-FAU detectives approached the vehicle and ordered MORGAN-GRAHAM out by name, to which he complied.

16. Search incident to arrest, a 9mm Glock Model 19 Gen 4 pistol, bearing serial number VVG836, equipped with a loaded magazine and with a round in the chamber, was recovered from the front of MORGAN-GRAHAM's waistband. The firearm also appeared to have a Glock Conversion Device, commonly referred to as a "switch," installed. I am aware that such devices are intended to convert semiautomatic firearms to fully-automatic firearms.

17. A "Glock Switch", known as a Glock Conversion Device, is considered a machinegun, under the National Firearms Act (NFA), 26 U.S.C. § 5845(b). Specifically, a machine gun is defined as any part or combination of parts, designed, and intended solely and exclusively for use converting a weapon into a machine gun. Glock Conversion Devices can be placed into a Glock, semi-automatic pistol, and convert the said firearm to a fully-automatic machinegun. Therefore, your affiant is aware that a Glock Conversion Device is a "machine gun" under the NFA. A "machine gun" is also considered a "firearm" under the NFA, pursuant to 26 U.S.C.

§ 5845(a). It is a violation of 26 U.S.C. § 5861(d) to receive or possess any “firearm,” as so defined under the NFA, if it is not registered to the receiver or possessor in the National Firearms Registration and Transfer Record (NFRTR).

18. In addition to the firearm, MORGAN-GRAHAM was wearing a male purse/shoulder bag. It is worth noting that within the last week, PBP-FAU detectives conducting surveillance of MORGAN-GRAHAM had seen him in possession with what appeared to be this same purse.

19. Search incident to arrest, investigators also searched this purse, and it contained a brick of suspected heroin/fentanyl, three bags of suspected crack cocaine, a bag of suspected raw fentanyl/heroin, a digital scale with powder residue, an extended magazine loaded with 9mm ammunition, surgical gloves, a ski-mask, and several empty baggies. It is worth noting that the digital scale was field tested and tested positive for the presence of cocaine. No user paraphernalia for heroin/fentanyl or crack cocaine was recovered.

20. **THE DEVICES** were recovered from MORGAN-GRAHAM. **DEVICE 1** was recovered from MORGAN-GRAHAM’s left hand, **DEVICE 2** was recovered from MORGAN-GRAHAM’s right front pocket, and **DEVICE 3** was recovered from MORGAN-GRAHAM’s right front pocket. Additionally, a total of approximately \$1881 in cash was seized from MORGAN-GRAHAM.

21. Investigators have reviewed publicly available court records, which show that MORGAN-GRAHAM’s criminal history includes the following felony convictions in the Criminal Division of the Allegheny County Court of Common Pleas:

- On or about October 30, 2018, Possession with Intent to Deliver a Controlled Substance (“PWID”), at Criminal Docket Number 6542-2018;

- On or about May 15, 2018, PWID, at Criminal Docket Number 13142-2017; and
- On or about May 15, 2018, PWID, at Criminal Docket Number 7880-2017.

22. I am aware that these offenses are felony offenses, punishable by more than one year of incarceration. Furthermore, MORGAN-GRAHAM would have also been so aware, because he received sentences of more than one year of incarceration in connection with these offenses.

23. Based on my training and experience and my knowledge of the facts and circumstances surrounding the recovery of the narcotics from MORGAN-GRAHAM, I believe those narcotics were possessed for distribution purposes and not for personal use. This belief is based on several factors, including the quantity of narcotics recovered, the manner in which they were packaged, the amount of cash recovered from MORGAN-GRAHAM, the presence of drug packaging paraphernalia such as the digital scale and empty baggies, MORGAN GRAHAM's possession of three cellular phones and a firearm, and MORGAN GRAHAM's criminal history.

**EVIDENCE COMMONLY STORED ON CELL PHONES AND OTHER
ELECTRONIC STORAGE THE DEVICES**

24. Based on my training and experience, I know that persons that often illegally possess firearms and narcotics often communicate with others using cellular devices phones, text messaging apps, and coded communications to interact with and do business with their customers, suppliers, confederates, and couriers. I also know that drug traffickers utilize multiple cell phones to evade law enforcement detection and that drug traffickers utilize firearms in furtherance of their illegal activities. Therefore, I know that evidence of drug crimes can be found in electronic media such as cell phones. Such evidence includes, but is not limited to addresses, telephone numbers, email and texts to confederates involved in the drug trade. Since drug dealers and users rely

heavily on cell phones, I know that evidence of their drug crimes can be found on cellular telephones. The communication between drug dealers and users can be either by placing a call or text messaging. Often times, contact lists or other numbers associated with the drug dealer's organization will be found and further illustrate the criminal conspiracy. This evidence is crucial for law enforcement to be able to identify and arrest all individuals involved in a particular narcotics sale.

25. Further, I am aware that individuals who illegally possess firearms and narcotics commonly use their cellular telephones to take exchange and retain "trophy" photographs and videos of their firearms, narcotics and or proceeds. Persons involved in narcotics trafficking often take photos of a "brand or stamp" of heroin they are currently distributing to send to the purchasers. Such persons, like law-abiding citizens, commonly take and exchange photographs and videos, using their cellular telephones, of themselves with their friends, relatives, and associates and keep the photographs on their cellular telephones. When they are taken, exchanged, or retained, such photographs and videos can be significant evidence, and can also lead to additional evidence.

26. As with most electronic/digital technology items, communications made from an electronic device, such as a cellular telephone, are typically saved or stored on **THE DEVICES**. Storing this information can be intentional, for example, by saving a text message, or a contact, or an email. Digital information can also be retained unintentionally. Traces of the path of an electronic communication, or of an internet search (for items such as electronic scales, or real properties for sale, or vehicles) may be automatically stored in many places on a cellular telephone. A forensic examiner often can recover evidence that shows when and in what manner a user of an electronic device, such as a computer or a cellular phone, used such a device. Electronic files or

remnants of such files can be recovered months or even years after they have been downloaded, stored, deleted, or viewed.

27. Your Affiant is aware, based upon my training and experience, that the following kinds of evidence have been recovered in a substantial number of cellular telephone searches executed in connection with investigations into the illegal possession of firearms:

- a) Contact lists; including telephone numbers, names and images associated with those numbers;
- b) Incoming and Outgoing call logs;
- c) Incoming and outgoing text messages (both SMS and MMS), including draft text messages, chats, Facebook messenger chats;
- d) Photographs; and
- e) Videos
- f) Metadata and physical location data
- g) Emails

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

28. Based on my knowledge, training, and experience, I know that electronic **THE DEVICES** can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on **THE DEVICES**. This information can sometimes be recovered with forensics tools.

29. There is probable cause to believe that things that were once stored on **THE DEVICES** may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

Forensic Evidence: Deleted Files, User Attribution

30. As further described in Attachment A, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how **THE DEVICES** were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on **THE DEVICES** because:

- Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration

information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage **THE DEVICES** or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

- Forensic evidence on a device can also indicate who has used or controlled **THE DEVICES**. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

- A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic **THE DEVICES** were used, the purpose of their use, who used them, and when.

- The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

- *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the **THE DEVICES**

consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of THE DEVICES to human inspection in order to determine whether it is evidence described by the warrant.

- Manner of execution. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

31. Based upon the foregoing, your Affiant respectfully requests that this Court issue a search warrant for **THE DEVICES** authorizing the search for and seizure of the information and material described in Attachment A.

The above information is true and correct to the best of my knowledge, information, and belief.

/s/ Marc Wilner
Marc Wilner
Special Agent - ATF

Sworn and subscribed before me, by telephone
pursuant to Fed. R. Crim. P. 4.1(b)(2)(A),
this 28th day of September, 2023.

HONORABLE CYNTHIA REED EDDY
United States Magistrate Judge

ATTACHMENT A

1. All records, information, and items evidencing who used the device and/or when and/or from where, or a violation Title 21, United States Code, Section 841(a), Title 18, United States Code, Sections 922(g) and 924(c) including:

- a. incoming and outgoing call and text message logs
- b. contact lists
- c. photo and video galleries
- d. sent and received text messages
- e. online searches and sites viewed via the internet
- f. online or electronic communications sent and received, including email, chat, instant messages and social media accounts
- g. sent and received audio files
- h. navigation, mapping, and GPS files
- i. telephone settings, including speed dial numbers and the telephone number for the subject telephone and related identifying information such as the ESN for the telephone
- j. call forwarding information
- k. messages drafted but not sent
- l. voice messages

2. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form. However, no real-time communications will be intercepted and searched during service.